EP3260: Machine Learning Over Networks
Computer Assignment 4
Due Date: March 15, 2023

Computer Assignment 4 - Sensitivity to outliers

Split "MNIST" dataset to 10 random disjoint subsets, each for one worker, and consider SVM classifier in the form of $\min_{\mathbf{w}} \frac{1}{N} \sum_{i \in [N]} f_i(\mathbf{w})$ with $N = 10$. Consider the following outlier model: each worker i at every iteration independently and randomly with probability p adds a zero-mean Gaussian noise with a large variance R to the information it shares, i.e., ∇f_i and $\mathbf{w}_{j,k}$ in the cases of Algorithm 1 and decentralized subgradient method of Lecture 6, respectively.

a) Run decentralized gradient descent (Algorithm 1) with 10 workers.

   Characterize the convergence against p and R.

   Propose an efficient approach to improve the robustness of Algorithm 1 and characterize its convergence against p and R.

b) Consider a two-star topology with communication graph (1,2,3,4)-5-6-(7,8,9,10) and run decentralized subgradient method.

   Characterize the convergence against p and R.

   Propose an efficient approach to improve the robustness to outliers and characterize its convergence against p and R.

c) Assume that we can protect only three workers in the sense that they would always send the true information. Which workers you protect in Algorithm 1 and which in the two-star topology, running decentralized subgradient method?